



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools
and Universities\)](#)

[International](#)

[Information Technology and
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security
Contacts](#)

[Emergency Services](#)

NORTH DAKOTA

Roof fire damages Wahpeton Cargill plant. A smoldering fire on February 24 damaged the roof of the Cargill plant in rural Wahpeton, North Dakota. Some plant workers were sent home for the day and others went to safe locations as firefighters from the Wahpeton and Dwight fire departments worked to extinguish a smoldering fire that spread through roof insulation, said the facility manager at the plant that produces high fructose corn syrup. The fire started in an area where contractors were attempting to create an access panel in the roof. Insulation began smoldering, and the fire spread through the insulation layer of the roof. Firefighters used thermal imaging to trace the path of the fire and eliminate problem spots. The Richland County Sheriff's Department issued a report on the fire about 1 p.m. At about 2:30 p.m. it appeared the fire had been put out and he anticipated the plant would be up and running again later in the afternoon. Source:

<http://www.inforum.com/event/article/id/309980/group/News/>

Corps of Engineers statement on James River flows. Due to abnormally high snow pack conditions in North Dakota, the Omaha District, U.S. Army Corps of Engineers (USACE) expects high inflows into Jamestown and Pipestem Reservoirs this spring. Pipestem Dam is a USACE project, while Jamestown Dam is a Bureau of Reclamation (Reclamation) project regulated by the Corps when the reservoir pool level reaches the flood control zone. The dams are located on the James River and Pipestem Creek just north of Jamestown. Current snow pack conditions are similar to previous high runoff years in 1997 and 2010, when the total runoff volume was 420,000 acre-feet and 350,000 acre-feet, respectively. USACE expects a similar runoff volume in 2011, although the runoff volume could be substantially altered, depending on additional snowfall or rainfall. USACE, Reclamation, and National Weather Service will continue to monitor snow pack conditions and will provide updated forecasts as conditions change. Source: http://www.ksibam.com/artman/publish/article_2973.shtml

REGIONAL

(Minnesota) FBI Says Robbery Suspect Hits 4th Metro Bank. With a mask and a small knife in hand, a man robbed a bank in Orono, Minnesota February 17, and FBI Agents said they believe it may be the same person who robbed three or four other banks in the metro area the past few weeks. FBI Agents said the First National Bank of the Lakes branch at 2445 Shadywood Road was robbed around 7:15 a.m. A bank employee arrived for work, and officials said the robber approached her from behind, told her he had a gun and to go into the bank. The employee told authorities she gave an undisclosed amount of money out of the night deposit safe to the man. She said the suspect left the bank through the front door. She was not hurt. The suspect is described as a white male, about 5 feet 9 inches tall, with a medium build. He was wearing dark clothing, along with a dark mask and gloves, white sneakers and carried a small blue, zippered bank bag. Source:

<http://kstp.com/article/stories/s1979532.shtml>

UNCLASSIFIED

(Minnesota) House agrees to lift ban on new nuclear power plants. Minnesota took a big step toward removing a ban on new nuclear power plants February 17 when the state house followed the senate's lead and voted to dump the 17-year-old moratorium. It marked the first time both houses had passed the controversial proposal in the same year. Still, the Republican-led effort has a ways to go. The governor has opposed it, demanding three criteria for his support. The house met one of them by adding a restriction against reprocessing spent fuel into weapons-grade plutonium. But the bill still lacks ratepayer protections and a lid on more nuclear-waste storage. While Republicans got some Democratic-Farmer-Labor support, the 81-50 vote fell short of the 90 supporters Republicans would need to override a veto by the governor. The senate passed a similar bill this month on a veto-proof 50-14 vote. Source: http://www.twincities.com/ci_17418021?nclick_check=1

(Montana) Corporate Air hit with second FAA citation. For the second time in 4 months, the Federal Aviation Administration (FAA) fined Corporate Air of Billings, Montana, for failing to repair problems with its airplanes. Corporate Air, which started business in Billings 30 years ago, faces total fines of about \$1 million for failing to follow FAA regulations. The week of February 14, FAA fined Corporate \$585,725 for allegedly flying a twin-turboprop cargo airplane at least 81 times between December 21, 2009 and February 4, 2010 when the plane had exterior corrosion. The company has 30 days to respond to the proposed fine. FAA said Corporate failed to detect the corrosion even though regulations require inspections of the aircraft after each flight. The company also failed to run required structural inspections for 4 years from March 2006 to February 2010, FAA said. A previous penalty in October involved a \$455,000 FAA fine for failing to fix a serious engine oil leak on a passenger airplane. Source: http://billingsgazette.com/news/local/article_b8f73c32-16d8-565d-9af5-1e052ac02ec7.html

NATIONAL

(Louisiana) Oil-spill investigators: 'This was an entirely preventable disaster. BP failed to keep a close watch on work done by the cement contractor at its doomed Macondo oil well, even though an audit had spotlighted problems with the firm, Halliburton Co., 3 years before the Deepwater Horizon disaster, according to the Presidential oil spill commission. The inadequate oversight may have proved deadly, the panel's chief investigator concluded February 17, because the "root technical cause" of the blowout in the well in the Gulf of Mexico off the coast of Louisiana that killed 11 workers and unleashed the spill April 20 was a failure of "the cement that BP and Halliburton pumped to the bottom of the well." In a 357-page report that expands on the panel's earlier accounts of the disaster, the commission's chief counsel, also said workers accepted implausible explanations for errant test readings that could have revealed problems with the cement. The chief counsel's report underscores the commission's January 11 conclusions that a series of technical failures contributed to the blowout, but all of them can be traced back to "an overarching failure of management." For instance, the commissioner faulted BP for "inadequately" supervising the cement job done by Halliburton, since the British oil giant had long raised concerns about the contractor's work performance. The commission previously documented concerns about the stability of the nitrogen-injected foam cement used to seal the Macondo well before BP temporarily stopped work at the site. A faulty cement job could allow channels or vulnerabilities for natural gas and oil to escape a well during the time between when it is drilled and when it is later hooked up to a production facility. Source: <http://www.houmatoday.com/article/20110218/WIRE/110219464/-1/sports?Title=Oil-spill-investigators-This-was-an-entirely-preven-table-disaster->

UNCLASSIFIED

INTERNATIONAL

China oil company says Libyan facilities attacked. China National Petroleum Corp. (CNPC) said its facilities in Libya were attacked, and that its employees have been evacuated back to China. A statement issued February 24 on CNPC's website mentions that its project and job site were under attack, prompting an order for all staff to withdraw. It did not mention the location of the facility or any other details. State-run CNPC said it has five subsidiaries and 391 Chinese staff in Libya. The first 24 workers were repatriated by February 24. The company said it was doing "everything possible to protect its projects and assets and ensure the safety of its employees." Source:

<http://www.businessweek.com/ap/financialnews/D9LJ33QO0.htm>

12 taxi drivers, fares killed in Mexican resort. A spate of attacks on taxis in the Mexican resort city of Acapulco has left 12 taxi drivers or passengers dead, police said February 20, just hours before the Mexican Open tennis tournament began. Taxi drivers have often been targeted for extortion or recruited by drug cartels to act as lookouts or transport drugs. The organizers of the largest tennis tournament in Latin America said in a statement the Mexican government has assured them that appropriate security measures have been taken for the event that started February 21. Police in Guerrero state, where Acapulco is located, said four suspects had been detained in relation to some of the attacks. The suspects had guns, a grenade, and a machete that police said may have been used to decapitate some of the victims. The attacks began February 18, when five taxi drivers were found dead in or near their vehicles. The murders continued February 19, when a driver was found bound and shot to death near his taxi, and two others were found dead of bullet wounds inside their vehicles. One of the drivers had been beheaded. On February 20, five cars were set afire and a man's body was found outside an apartment building. Source:

http://www.msnbc.msn.com/id/41699216/ns/world_news-americas/

Milan airport terminal evacuated after shooting. A terminal at Milan, Italy's Malpensa airport was evacuated February 21 when a man smashed his car into the terminal building and was shot by a police officer after trying to stab him, a security source said. "A Tunisian man ... who was in a car with his wife and three children tried to smash into the terminal," the source told Agence France-Presse. "He then got out of the car with a knife in his hand and threatened a police officer," the source said. "The officer tried to calm him and escort him out of the terminal. When the man threw his knife at the officer, the officer shot him in the foot." All flights departing from Malpensa were suspended after the incident, while arrivals continued as normal, ANSA news agency reported. Source:

<http://news.asiaone.com/News/Latest+News/Relax/Story/A1Story20110221-264705.html>

Major oil companies evacuate employees. Global oil companies said February 21 that they were making plans to evacuate employees in Libya after some operations there were disrupted by political unrest. Eni of Italy, said in a statement that it had begun repatriating "nonessential personnel" and the families of its employees. The Norwegian energy company Statoil, which operates in Libya in partnership with Repsol of Spain and Total of France, said it would close its office in Tripoli, and that a handful of foreign workers were leaving. OMV of Austria, which produces about 34,000 barrels of oil per day in Libya, said it planned to evacuate 11 workers and their families, leaving only essential staff. The British oil company BP, which has only exploration operations in Libya, said it was planning to evacuate some of its 40 foreign workers, mostly from Tripoli. It also said it had suspended

preparations for a drilling project because employees of a contractor had been evacuated. Source: <http://www.thepeninsulaqatar.com/latest-news/143358-major-oil-companies-evacuate-employees-.html>

Mexican drug gangsters menace natural gas drillers. Gunmen claiming to represent a powerful drug cartel have threatened to attack isolated natural gas well drillers unless they pay to operate in parts of northern Mexico, two industry sources said February 15. The gunmen warned workers they would be killed unless their employer paid protection money to Zetas, a feared drug gang, a senior executive of the company overseeing the construction of the wells told Reuters. The threats are a new twist in Mexico's bloody drug war, which is hitting businesses near the United States-Mexico border. In one case, the suspected drug gang demanded 10 percent of what Pemex was paying for the gas contract, the company executive said. Security at the well sites is under review, but no drilling has gone ahead there, the executive said. An external consultant employed at Pemex's Mexico City headquarters confirmed the events. There are believed to be other gangs threatening gas fields, but only the instances involving gunmen identifying themselves as Zetas have been confirmed by company sources. Source: http://news.yahoo.com/s/nm/20110215/wl_nm/us_mexico_drugs_energy

BANKING AND FINANCE INDUSTRY

New type of financial malware hijacks online banking sessions. A new type of financial malware has the ability to hijack customers' online banking sessions in real time using their session ID tokens. OddJob, which is the name Trusteer gave to this trojan, keeps sessions open after customers think they have "logged off," enabling criminals to extract money and commit fraud unnoticed. This is a completely new piece of malware that pushes the hacking envelope through the evolution of existing attack methodologies. It shows how hacker ingenuity can side-step many commercial IT security applications traditionally used to defend users' digital and online monetary assets. Trusteer has been monitoring OddJob for a few months, but had not been able to report on its activities until now due to ongoing investigations by law enforcement agencies. These have just been completed. Trusteer's research team reverse engineered and dissected OddJob's code methodology, right down to the banks it targets and its attack methods. Financial institutions have been warned OddJob is being used by criminals based in Eastern Europe to attack their customers in several countries including the United States, Poland, and Denmark. Source: http://www.net-security.org/malware_news.php?id=1636

Fake FDIC emails distribute trojan. M86 Security warned of a new spam run that generates malware-carrying e-mails purporting to come from the Federal Deposit Insurance Corporation (FDIC). M86 said the e-mails are sent by Cutwail, a spam botnet, which at its peak accounted for more than 40 percent of the daily junk mail traffic. The rogue notifications bear a subject of "Important information for depositors of Federal Deposit Insurance Corporation" and carry an attachment called FDIC_Document(dot)zip. The message contained within reads: "Attention! Dear Depositor, this message was sent to you as you had indicated this e-mail address as a contact, by opening an account in your bank department. In order to inform you about the news concerning current business activity of the Company on a timely basis, please, look through the last important changes in current regulations of endowment insurance procedure. Please, refer to more detailed information in the attached document." One giveaway the e-mails are fake is the From field lists a (at)ups(dot)com address, a remnant from a fake UPS campaign the spammers forgot to change. The malicious

UNCLASSIFIED

executable found inside the attached archive is a variant of SpyEye, a sophisticated banking trojan used to steal financial and personal data from victims. Source:

<http://news.softpedia.com/news/Fake-FDIC-Emails-Distribute-Trojan-184761.shtml>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

NRC weighs new study of cancer risks near nuclear plants. Federal researchers with the Nuclear Regulatory Commission (NRC) said February 24 that a proposed study of cancer risks around nuclear facilities could improve the public's trust in existing evidence that radiation doses emitted from those plants are not harmful. The study's senior project manager told a committee of 19 independent experts organized through the National Academy of Sciences that the rationale for undertaking such a study would be to obtain credible, and updated, information for the public about possible cancer risks from nuclear plants. The last study on the issue was done in 1990. Millstone Power Station in Waterford is one of 104 nuclear facilities across the country that would be included if the experts from the NRC and the national academy decide to go forward with a comprehensive study. By partnering with the academy, the NRC would update a 1990 study by the National Cancer Institute that found no increased risk of death from cancer for those living in the 107 counties either containing or located near nuclear power reactors that were operating before 1982. The 1990 U.S. study on possible cancer risks from nuclear plants was undertaken after a study in the United Kingdom found "significant excess" of childhood leukemia around certain nuclear facilities there. The director of the NRC's Office of Nuclear Regulatory Research said the goal of the study would be to provide public assurance. Source: <http://www.theday.com/article/20110225/BIZ02/302259874/-1/BIZ>

COMMERCIAL FACILITIES

(Texas) Kilgore hotel evacuates after meth lab fire. A Kilgore, Texas hotel was evacuated February 16 after a meth lab caught fire, resulting in three Kilgore residents behind bars, and the seizure of drugs, counterfeiting equipment, counterfeit checks, money, and forged identification. Kilgore fire and police officials were dispatched to America's Best Value Inn and Suites in the 3200 block of U.S. 259 at midnight in connection with a fire that started in one of the rooms, a Kilgore police spokesman said. "After the hotel was evacuated and the fire was extinguished within the room, the cause of the fire was soon discovered to be a methamphetamine lab," he said. Two suspects were arrested at the scene and charged with possession of a controlled substance; the third was charged with manufacturing and delivery of a controlled substance. The spokesman said 4.1 grams of methamphetamine were found in the room along with lab equipment and chemicals commonly used in manufacturing the drug. A total of 16 grams of meth was found on the suspects. Source: <http://www.ketknbc.com/news/kilgore-hotel-evacuates-after-meth-lab-fire>

(Nevada) Police: Man opened fire on passing cars in Vegas. Police said a man parked a red sport utility vehicle near a Las Vegas, Nevada freeway and opened fire on passing cars, wounding one person before being shot by officers and arrested. A police officer said the shooting happened about 2:30 p.m. February 17 on Interstate 15 just south of the Las Vegas Strip. The Las Vegas police officer said a police officer shot the gunman, described as a man in his 30s. She said the suspect's injuries aren't life-threatening, and that two other people were in police custody. The police officer said the

UNCLASSIFIED

person wounded by the gunman also has non-life threatening injuries. A Nevada Highway Patrol Trooper said southbound I-15 was briefly shut down, but quickly reopened with exits and entrances closed near the scene at Blue Diamond Road. Source: <http://www.buffalonews.com/wire-feeds/24-hour-national-news/article344853.ece>

COMMUNICATIONS SECTOR

Powerful solar flare disrupts ground communications. A powerful solar flare that has triggered one of the largest space weather storms in at least 4 years has disrupted some ground communications, University of Colorado-Boulder (CU) scientists said. Solar coronal mass ejections, such as February 15's Class X flare, can cause a variety of socioeconomic and safety issues such as disruption of airline navigation systems, satellite operations, power grids and safety of airline crews and astronauts. "The sun is coming back to life," the director of CU's Laboratory for Atmospheric and Space Physics said. The National Oceanic and Atmospheric Administration said several more strong ejections may reach Earth's atmosphere by the end of the week of February 14. "We understand much more about what is happening and can build more robust systems to withstand the effects," the director said. "It will be interesting to see how well our technological systems will withstand the rigors of space weather as the sun gets back to higher activity levels." Source: http://www.denverpost.com/breakingnews/ci_17422606

New wireless tech jams GPS. The Deputy Secretary of Defense has raised concerns with the Federal Communications Commission (FCC) about a new technology used by a company called LightSquared that jams military and civilian Global Positioning System (GPS) signals. The Federal Aviation Administration (FAA) shares the Pentagon's worries. The head of Air Force Space Command disclosed these concerns at the Air Force Association winter conference February 17. He told reporters an unnamed GPS company had tested its gear and found that LightSquared's towers built to generate a 4G wireless network completely jammed reception. FCC recently granted a conditional license to the company to begin building its network using L-band spectrum, "right next to" the GPS signal, he said. The conditional license requires Light Squared to prove it does not jam other signals. The company would operate only in the United States. FCC has told the company to work with the federal government and the GPS industry in a working group to find answers to the jamming problems. The members and goals of the working group are to be presented to FCC by February 25. Source: <http://www.dodbuzz.com/2011/02/17/new-wireless-tech-jams-gps/>

CRITICAL MANUFACTURING

Toyota recalling 2.17 million vehicles in U.S. Toyota Motor Corp. recalled 2.17 million vehicles in the United States February 24 to address accelerator pedals that could become entrapped in floor mats or jammed in driver's side carpeting, prompting federal regulators to close its investigation into the embattled automaker. The U.S. Department of Transportation said it had reviewed more than 400,000 pages of Toyota documents to determine whether the scope of the company's recalls for pedal entrapment was sufficient. "As a result of the agency's review, (the National Highway Traffic Safety Administration[NHTSA]) asked Toyota to recall these additional vehicles, and now that the company has done so, our investigation is closed," an NHTSA administrator said. Toyota has now recalled more than 14 million vehicles globally to fix gas pedals and other safety problems since 2009.

UNCLASSIFIED

U.S. regulators said earlier in February 2011 that electronic flaws were not to blame for reports of sudden, unintended acceleration. Source: <http://www.msnbc.msn.com/id/41756436/ns/business-autos/>

Ford to recall F-150 pickups over air bags. Under government pressure, Ford Motor Co. said February 23 it will recall nearly 150,000 F-150 pickup trucks to fix air bags that could deploy without warning, a fraction of the vehicles the government contends should be called back and repaired. The recall covers trucks from the 2005-2006 model years in the United States and Canada for what Ford calls a “relatively low risk” of the air bag deploying inadvertently. The government, however, has urged the company to recall 1.3 million F-150s from the 2004-2006 model years, citing 77 injuries from air bags deploying accidentally. The recall is being closely watched because Ford’s F-Series pickup truck is the best-selling vehicle in America. The National Highway Traffic Safety Administration (NHTSA) has been investigating the air bag issues for more than a year. In May 2010, Ford told the government that the problems did not “present an unreasonable risk to vehicle safety” because there was a low rate of alleged injuries and the air bag warning lamp provided an “obvious warning” to drivers. Ford told NHTSA in May that some drivers reported injuries that included burns from contact with the air bag, bruises, neck and back pain, and minor cuts. “Two customers reported broken or chipped teeth and two reported fractures of the extremities (elbow or arm),” wrote the director of Ford’s automotive safety office. The NHTSA’s acting director of defect investigations, wrote in a memo November 24, 2010 that the agency knew of 238 cases in which the air bags deployed inadvertently and noted that Ford made production changes to the trucks in 2006 and 2007 to fix the air bag wiring and other issues. The memo said that Ford did not believe the issue “warrants any corrective action” because the number of reports and incidents were low, owners received “adequate warning” from the air bag warning light and the “resulting injuries are minor in nature.” The government said Ford should conduct a recall “to remedy this defective condition.” Source: <http://www.msnbc.msn.com/id/41733165/ns/business-autos/>

Sno-Tek snow blowers recalled by Liquid Combustion Technology Due to laceration hazard. Liquid Combustion Technology, LLC (LCT), of Travelers Rest, South Carolina, issued a recall February 17 of about 1,500 Sno-Tek snow blowers. The manufacturer was Ariens, of Brillion, Wisconsin. The snow blower’s engine is missing a safety shield above the side mounted electric starter, posing a laceration hazard to consumer’s fingers. No injuries/incidents have been reported. The snow blowers were sold at Home Depot and Ariens authorized dealers nationwide from August 2010 through September 2010. Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml11/11137.html>

LEM Products recalls food dehydrators due to fire hazard. LEM Products, of Harrison, Ohio, issued a recall February 16 of about 3,500 food dehydrators with digital timers. The screws that secure the motor to the back panel can come loose, causing the motor to fall on the heating element. This poses a fire hazard. LEM has received five reports of motors falling on the unit’s heating element resulting in smoke or fire contained in the unit. No injuries have been reported. The food dehydrators were sold at mass merchandisers and retailers nationwide and online at [www\(dot\)lemproducts\(dot\)com](http://www.lemproducts.com) from August 2010 through December 2010. Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml11/11131.html>

Atico International USA recalls heaters due to fire hazard. Atico International USA, Inc. of Fort Lauderdale, Florida, issued a recall February 16 of about 92,000 TrueLiving Heater Fans and Portable

UNCLASSIFIED

Quartz Radiant Heaters. The importer/retailer was Dollar General Stores of Goodlettsville, Tennessee. The heaters have caught fire, posing a fire hazard to consumers. Atico has received 8 reports of the A14B1053 Heater Fan overheating and 21 reports of the A14B0979 Quartz Heater overheating. Reports for the A14B1053 Heater Fan included one report of damage to an electrical outlet and wall, and one report of flames coming out of the front of the unit. Reports for the A14B0979 Quartz Heater included damage to the heater's plug, one report of flames coming from a control knob, and one report of a consumer receiving minor burns to the hand. For both products, reports included incidents of smoke and melting of the plastic casing. The heaters were sold exclusively at Dollar General Stores from September 2010 to December 2010. Source:

<http://www.cpsc.gov/cpsc/pub/prerel/prhtml11/11130.html>

DEFENSE/ INDUSTRY BASE SECTOR

(Texas) **Defense contractor offers hefty reward in thefts.** Aero Components Inc. is offering \$10,000 for a conviction in the case and return of the stolen materials. Three men broke into a gated, locked exterior storage facility in south Fort Worth, Texas, three times in a 24-hour period. The first break-in was at about 5 a.m. February 13. The men returned at 8 p.m. and then again February 14 at 5 a.m. The company manufactures aircraft parts for the Department of Defense, Lockheed Martin, and Bell Helicopter, to name a few. The theft of the aluminum toolings, which are essentially the parts' form, could mean up to a \$10,000 loss and a possible delay in building some parts. The private company paid to monitor the security cameras during off-hours missed all three thefts. The Fort Worth Police Department is investigating the thefts but declined to comment because the investigation is in its preliminary stages. The stolen items are used in aircraft parts but do not pose a security risk, but the Pentagon was notified because the theft could slow production of some parts. Source:

<http://www.nbcdfw.com/news/local/Defense-Contractor-Offers-Hefty-Reward-in-Thefts-116870193.html>

EMERGENCY SERVICES

Tunnel detection task force speeds sensors, robots to border. A federal task force organized to halt the construction of illegal tunnels being built underneath the U.S.-Mexico border has begun deploying ground sensors and robots in the Southwest. With 129 tunnels detected under U.S. borders since 1990, DHS, U.S. Northern Command, the Army Corps of Engineers, and other agencies formed the rapid reaction tunnel detection joint capability technology demonstration in 2010. Its first task was to deploy a series of passive seismic sensors, which can detect movement underground at hotspots. That happened within months of the organization's formation, the program's operational manager said. Leadership does not want to wait "3 years" before deploying technology, she added. We "want to get something in the field now — this year," she said. Next will be tethered robots sent into tunnels for mapping and situational awareness. They will be inserted through 8-inch-wide boreholes drilled down to underground cavities. They come equipped with a suite of sensors, including electro-optical, infrared, and chemical-biological to detect weapons of mass destruction. Mapping can reveal entrances that emerge on private property, thus allowing law enforcement agencies to obtain search warrants, she said. An untethered robot that can independently move in tunnels is under development, she said. Source:

UNCLASSIFIED

<http://www.nationaldefensemagazine.org/archive/2011/March/Pages/TunnelDetectionTaskForceSpeedsSensorsRobotstoBorder.aspx>

(Ohio) Video conferencing technology is making law enforcement's job easier. All around the country, police agencies have had to cut their staffs during the recession. Courtrooms are increasingly using video conferencing, mainly for suspects in custody awaiting their initial appearance in municipal court. Video conferencing has become much easier to implement in recent years and much more cost-effective, a Painesville, Ohio clerk of court said. There are now five OHio cities utilizing it: Willoughby, Willoughby Hills, Eastlake, Willowick, and Wickliffe. Each morning, Willoughby's bailiff checks in with the police departments to see whether there are any people in custody that day. Then officials build an arraignment list, any defendants who can be arraigned via video talk to the judge right from their jail cell. Defense attorneys can participate at the jail or in court. Initially, some police officers were hesitant to participate in video arraignments because of the initial paperwork involved. "But that was quickly dispelled after they found out how much easier it was," an official said. "The police officers are the ones who really make it work." Source: <http://news-herald.com/articles/2011/02/22/news/doc4d62843d44470830272864.txt?viewmode=fullstory>

FBI: Web-based services hurting wiretapping efforts. Web-based e-mail, social-networking, and peer-to-peer services are frustrating law enforcement wiretapping efforts, a lawyer for the FBI told lawmakers February 17, but she did not offer concrete ideas on how to fix the problem. The President's administration is debating ways to deal with Web-based services not covered by traditional wiretap laws, including incentives for companies to build in surveillance capabilities, the general counsel at the FBI said. Many Internet services are not covered by the Communications Assistance for Law Enforcement Act (CALEA), which requires traditional telecom carriers to allow law enforcement agencies real-time access to communications after a court has issued a wiretap order, she told members of a subcommittee of the U.S. House of Representatives Judiciary Committee. The FBI is concerned law enforcement investigations are being compromised by the lack of wiretap capability on some Web-based services and encrypted mobile telephone traffic, the FBI general counsel said. The American Civil Liberties Union has argued that expanding wiretapping capabilities would harm the Internet. Source: http://www.pcworld.com/businesscenter/article/219984/fbi_webbased_services_hurting_wiretapping_efforts.html

(California) San Jose officials warn of massive police and fire layoffs. San Jose, California city officials warned the week of February 14 that they could lay off as many as 349 police officers and 145 firefighters, slashing close to a quarter of the city's public safety employees. The city is also looking at millions of dollars in other cuts, including shutting off neighborhood streetlights for much of the night and eliminating some gang-prevention programs. Last year, San Jose laid off 49 firefighters, and this is the second year in a row the police department has faced layoffs. The scenarios presented at preliminary budget sessions were based on the assumption the city would not extract concessions from public employee unions. But it is now clear that even with concessions, the layoffs will be severe. City officials said the looming \$110 million deficit projection must be made up through a combination of layoffs, concessions, program cuts, and pension reform. A spokesman for the city manager's office said that even if all 11 unions agree to 10 percent concessions in total compensation, the police department could still lose 237 positions, while firefighters could lose 82.

UNCLASSIFIED

UNCLASSIFIED

Citywide, nearly 60 positions are potentially on the chopping block, he said. The final decisions on layoffs are expected to be made during council budget sessions in June. Source:

http://www.mercurynews.com/crime-courts/ci_17397188

EPA and U.S. Coast Guard step up efforts to protect U.S. waters. The U.S. Environmental Protection Agency (EPA) and U.S. Coast Guard (USCG) have signed a memorandum of understanding (MOU) to work together to protect people's health and the environment. The MOU outlines steps the agencies will take to better coordinate efforts to prevent and enforce against illegal discharges of pollutants from vessels, such as cruise ships and oil tankers. Under the MOU, USCG has agreed to incorporate components of EPA's vessel general permit program into its existing inspection protocols and procedures to help the United States address vessel pollution in U.S. waters. The MOU creates a framework for improving EPA and USCG cooperation on data tracking, training, monitoring, enforcement, and industry outreach. The agencies have also agreed to improve existing data requirements so that information on potential violations observed during inspections can be sent to EPA for evaluation and follow-up. Source: <http://coalgeology.com/epa-and-u-s-coast-guard-step-up-efforts-to-protect-u-s-waters/13904/>

ENERGY

Hydrofluoric acid risk at oil refineries. Oil industry documents filed with the federal government reveal that an accidental release of a lethal chemical used in 50 aging refineries across the country could prove devastating, with 16 million Americans living within range of toxic plumes that could spread for miles. Los Angeles, Philadelphia, Minneapolis, New Orleans, and the stretch of Texas coastline known as "Refinery Row" are among the at-risk areas cited in the documents. Citing homeland security concerns, the government keeps the industry filings under close guard in Washington, D.C. They were reviewed as part of a joint investigation by ABC News and the Center for Public Integrity. According to the industry's worst-case scenario documents, a release of the chemical could endanger entire communities. Even though one-third of the oil refineries in the United States are using the chemical, a spokesman told ABC News that the industry has long avoided demands from safety advocates and from the union that represents refinery workers that it explore safer options. Officials at the U.S. Chemical Safety Board have warned that while the refinery industry has been painting a rosy picture of the conditions at their facilities, it has compiled a disconcerting track record. As the nation's 150 refineries have aged, there have been an increasing number of fatal, or near-fatal, incidents. Source: <http://abcnews.go.com/Blotter/hydrofluoric-acid-risk-oil-refineries/story?id=12985686>

FOOD AND AGRICULTURE

(Arkansas) USDA recalls meat from Ark. farm. The U.S. Department of Agriculture's Food and Safety Inspection Service (FSIS) has recalled various meat and poultry products sold at Petit Jean Farm in Morrilton, Arkansas. The meat products were recalled because they did not get a federal inspection. The recall includes products sold under the brand names "Meadow Lamb," "Meadow Beef," and "Petit Jean Farm." The products were sold through the Internet, as well as distributed at local markets and restaurants in Arkansas. Source: <http://www.4029tv.com/news/26992992/detail.html>

UNCLASSIFIED

FBI warns of fertilizer purchases for explosives. The FBI is reminding farm supply stores and other businesses across the United States to keep an eye out for suspicious purchases of fertilizer and other substances that can be used to make explosives. An FBI spokesman in Denver said February 24 that the FBI sent letters warning firms to watch for suspicious behavior by buyers and for unusually large purchases of certain fertilizers, pesticides, and other combustibles. ABC News first reported February 24 that letters had been sent to businesses around the country. An official from the FBI field office in Denver said the office sent letters to about 100 businesses in Colorado and Wyoming. The letter and an accompanying flier urge businesses to be aware of buyers with little knowledge of crops or fertilizers, large purchases of fertilizers containing ammonium nitrate out of season, and buyers paying with large amounts of cash or using rental vehicles to transport large amounts of fertilizer. Similar letters have been sent by FBI offices around the country to swimming pool firms and beauty supply stores. Source: http://www.laramieboomerang.com/articles/2011/02/25/ap-state-wy/co_terror_bomb_plot_fbi_warning.txt

Chicken and noodle product recall. Cedarlane Natural Foods, Inc., a Los Angeles, California, establishment, recalled about 1,050 pounds of chicken and noodle products, the U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) announced February 23. These products are misbranded because the USDA mark of inspection does not appear on the package labels available to consumers. The products subject to recall include: Cases containing six 16-ounce trays of "Wholesome Home Chicken & Noodles." The sell-by date "09/21/11" is ink jetted on the side of each case, and the Julian date "10264" can be found on the label of each 16-ounce tray. The distributor discovered the problem and notified Cedarlane, who then notified FSIS. It was determined the USDA mark of inspection was dropped from labels for this particular production day due to a printing error. Source: http://imperialvalleynews.com/index.php?option=com_content&task=view&id=9577&Itemid=1

WADA seeking information from China on beef tainted with steroids. The World Anti-Doping Agency (WADA) has asked China for information on the use of steroids in raising cattle after some athletes blamed their positive doping tests on tainted beef. The director general of WADA said February 22 that "there seems to be some evidence" that Chinese cattle may have been stimulated with steroids. A recent study by a WADA-accredited lab in Germany found that 22 of 28 travelers returning from China tested positive for low levels of clenbuterol, probably from food contamination. Source: <http://www.baltimoresun.com/sports/nationworld/wire/sns-ap-wada-china-tainted-beef,0,2636857.story>

China on alert for leather protein in milk supply. China warned dairy producers that inspectors are on alert for fresh milk tainted with the industrial chemical melamine and another toxic substance extracted from leather scraps. Both additives — melamine and hydrolyzed leather protein — would make dairy products made with watered-down milk appear to have normal amounts of protein. Infant formula tainted with melamine killed 6 children in China in 2008 and sickened more than 300,000. The ministry of agriculture said in a undated notice posted to the Web site of the state council, China's cabinet, that authorities will carry out 6,450 random checks on fresh milk in 2011 — underscoring official concerns dairy producers may still be trying to use illegal and dangerous methods to boost the protein content of their milk. All the tests will check for melamine, and 30

UNCLASSIFIED

percent will look for hydrolyzed leather protein. To find out if the substance has been added to dairy, authorities look for telltale leather-curing residues. The protein extracted from cow leather is not known to be dangerous to human health, but the curing chemicals are. The China Daily newspaper said the chemicals could be fatal for children in high doses and put adults at risk for osteoporosis.

Source: <http://www.google.com/hostednews/ap/article/ALeqM5j0e-HWmR3eVzrkHHz8ZG6PRfVL5Q?docId=161fccd8368b476c9ffec82200fbfea2>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Bill proposes chief security officers at federal agencies. New cybersecurity legislation before Congress calls for each federal agency to appoint a dedicated chief information security officer (CISO) to ensure the federal government is complying with cybersecurity regulations. The “Cybersecurity and Internet Freedom Act of 2011” — introduced by U.S. Senators from Connecticut, Maine, and Delaware — spells out the role of CISOs within federal agencies and outlines how federal agencies should better manage security both inside organizations and across the federal government. According to the bill, CISOs will, like Chief Information Officers (CIOs), be given the authority and a budget to perform their duties, first and foremost of which will be to ensure compliance with the security measures they set up within each agency. They also will designate a series of security controls that can be “continuously monitored” to ensure an agency is complying with its own regulations. According to the legislation, CISOs will be reporting to the director of the NCCC, who they must work with not only on security incidents affecting each agency, but also on ones that affect the government that are not under an agency’s jurisdiction, according to the bill. Source: http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=229219377&cid=RSSfeed_IWK_All

(Texas) Saudi national arrested on terror charge to make court appearance. A Saudi national arrested for allegedly researching and acquiring chemicals to make a bomb was expected to make his initial appearance February 25 in a federal court in Lubbock, Texas. The 20-year-old who attended school near Lubbock allegedly researched several possible targets, including the Dallas home of a former U.S. President along with nuclear power plants and hydroelectric dams. The suspect was arrested on a federal charge of attempted use of a weapon of mass destruction in connection with his alleged purchase of chemicals and equipment necessary to make an improvised explosive device, the Justice Department said. He faces a maximum sentence of life in prison and a \$250,000 fine if convicted of attempted use of a weapon of mass destruction, officials stated. According to court records, the man conducted online research into how to construct an improvised explosive device using several chemicals as ingredients. He has also “acquired or taken a substantial step toward acquiring most of the ingredients and equipment” needed for the bomb, documents said. Authorities said the man described his desire for violent jihad and martyrdom in blog postings and a personal journal. Source: <http://www.cnn.com/2011/CRIME/02/25/us.terror.arrest/>

U.S. lawmakers consider ways of arming U.S. agents in Mexico after killing of ICE agent. U.S. lawmakers on both sides of the aisle are weighing actions to allow U.S. agents working in Mexico to be armed after a drug gang killed an unarmed U.S. immigration agent and wounded another. U.S.

UNCLASSIFIED

UNCLASSIFIED

agents have not been allowed to carry weapons in Mexico since a 1990 agreement. But their safety has been increasingly in jeopardy ever since the Mexican president declared war on the drug cartels when he took office in December 2006. Two U.S. Immigration and Customs Enforcement agents were shot on a federal highway while traveling in the northern state of San Luis Potosi en route to Mexico City February 15. The area is at the center of a power struggle between two rival drug gangs. One agent was killed, the first murder of a U.S. agent in the line of duty during Mexico's drug war. Source: <http://www.foxnews.com/politics/2011/02/23/lawmakers-consider-proposal-arming-agents-mexico-ice-attack/>

(Texas; Colorado; California) FBI: Lubbock college student from Saudi Arabia targeted Bush's Dallas home in bombing plot. A 20-year-old Saudi Arabian national arrested by the FBI in Lubbock, Texas, for allegedly plotting to carry out terrorist attacks, also allegedly targeted the Dallas home of the 43rd U.S. President, documents show. The Saudi citizen was arrested February 23 and was scheduled to appear before a federal judge in Lubbock February 25. Agents also found lists of various targets, including reservoir dams in Colorado and California, and nuclear power plants. According to an arrest warrant affidavit, FBI agents learned of the man's alleged plotting February 1, when a chemical supplier reported a suspicious attempted purchase of concentrated phenol. Phenol can be used to make explosives. The suspect had successfully purchased concentrated nitric and sulfuric acids in December. He also allegedly purchased many other items, including a gas mask, a haz-mat suit, a soldering iron kit, glass beakers and flasks, wiring, a stun gun, clocks, and a battery tester. A spokesman said the terrorism investigation is ongoing, but "the federal complaint contains no allegations that he received direction from or was under the control of a foreign terrorist organization. We are confident that we have eliminated the alleged threat by [the accused]," he said. The suspect was lawfully admitted into the United States in 2008 on a student visa, and is enrolled at South Plains College near Lubbock. In online blog entries agents found, the man allegedly wrote of his plans to carry out violent jihad, or holy war, in the United States. The affidavit also alleged he conducted research indicating he considered using infant dolls to conceal explosives, and considered targeting of a nightclub with an explosive concealed in a backpack. A search of his Lubbock residence revealed a journal, which showed he had been allegedly plotting for years. Source: <http://www.dallasnews.com/news/state/headlines/20110224-fbi-lubbock-college-student-from-saudi-arabia-targeted-bushs-dallas-home-in-terror-plot.ece>

Phishers target EDU email users. Phishers are targeting university students with e-mails that pose as notifications from the system administrator claiming their (dot)edu e-mail accounts have exceeded the allowed storage quota. According to researchers from M86 Security, the attack was timed to coincide with students returning to school. An exceeded storage limit might sound plausible for students who have not checked their (dot)edu mailboxes in a while and left e-mails and spam to pile up. One phishing e-mail intercepted by the vendor read: "Your mailbox has exceeded the storage limit set by the administrator, you may not be able to send or receive new mail until you Re-validate your mailbox. To Re-validate and upgrade your mailbox please click here." Another one is more targeted and specifies the name of the university's Web service and how big the storage quota is. The actual phishing page suggests an inexperienced attacker. It displays a form created with an automatic tool, asking for full name, e-mail address, user name and password. According to the M86 researchers who also uncovered the unprotected admin panel, despite the poor quality of the phishing page, the attack still managed to claim many victims. Source: <http://news.softpedia.com/news/Phishers-Target-EDU-Email-Users-186067.shtml>

UNCLASSIFIED

Iranians hack into VOA website. Iranian computer hackers February 21 hijacked the Web site of the Voice of America (VOA), replacing its Internet home page with a banner bearing an Iranian flag and an image of an AK-47 assault rifle. The group called on the United States' Secretary of State to "hear the voice of oppressed nations." The banner stated "we have proven that we can." The message called on the United States to "stop interfering in Islamic countries." It then listed 90 more VOA Web sites it claimed also had been hacked. A State Department spokesman could not be reached for comment. An administration official said the group identified with the banner is known as the Iranian Cyber Army. VOA operates a global network of news and information outlets that reflect official U.S. foreign policies. It broadcasts, through radio, television, and the Internet to scores of nations around the world. Little is known about the hacking group. It was credited with hacking and defacing Twitter in December 2009, replacing the social networking site's home page with a message the site was hacked by the Iranian Cyber Army. Source: <http://www.washingtontimes.com/news/2011/feb/21/iranian-hackers-break-voa-deface-web-sites/>

(New York) Explosive detonates in county building. A homemade explosive device went off about 9:45 a.m. February 17 at the Erie County Board of Elections building in Buffalo, New York. No one was hurt, but everyone inside evacuated. The device was set off on the same floors that house the Erie County Sheriff's Professional Standards Unit, and it prompted a 1-hour evacuation and closure of West Eagle Street and Delaware. Investigators believe someone deliberately set off some type of a paper-wrapped explosive. A lieutenant from the Erie County Sheriff's office said, "We believe it is a device something in the neighborhood of an M-80, along that nature, slightly bigger than people may be accustomed to consumer fireworks." A mark on the wall shows where it went off in the stairwell between the fourth and fifth floors. The explosion did not do much damage. The halls are already in a state of disrepair. The building was originally supposed to be demolished soon, but that plan is on hold. Source: <http://www.wivb.com/dpp/news/crime/Explosive-detonates-in-county-building>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Site to highlight social networks' security soft spots. Security researchers have set up a site designed to prod social networking Web sites into practicing what they preach about web security. Socialnetworksecurity.org, which aims to publish details of security vulnerabilities on Web 2.0 sites such as Xing or Facebook, was set up the weekend of February 19 by security researchers frustrated with a lack of response from sites about the problems they discovered. Many of the vulnerabilities unearthed fall into the category of cross-site scripting vulnerabilities, some of which (in the case of bugs on Xing and Jappy.de, for example) have already been fixed. Separately, an insecure script on Facebook creates a mechanism to make more convincing phishing attacks. This bug remains live, Socialnetworksecurity.org warns. The German-based team behind the website, who wish to remain anonymous, want to push vendors into becoming more responsible about security bugs. At a first step they want Web 2.0 to establish a security-related contact form, and to allow submission of confidential security-related problems via encrypted e-mail. Source: http://www.theregister.co.uk/2011/02/22/social_network_insecurity/

The unintended kill switch in Bind. The developers of the Bind server software have warned of a security problem that could prevent DNS servers from responding to requests. This is a serious

problem, as many of the central DNS servers on the Internet use Bind, and hardly anything works without domain name resolution. However, the developers said no public exploits have so far been found. A domain's master servers are vulnerable while they are performing an incremental zone transfer — a type of DNS zone transfer – or a dynamic update. The relevant security advisory lists versions 9.7.1-9.7.2-P3 as being affected. Source: <http://www.h-online.com/security/news/item/The-unintended-kill-switch-in-Bind-1196567.html>

Flash drives dangerously hard to purge of sensitive data. In research that has important findings for banks, businesses, and security experts, scientists have found computer files stored on solid state drives are sometimes impossible to delete using traditional disk-erasure techniques. Even when the next-generation storage devices show files have been deleted, as much as 75 percent of the data contained in them may still reside on the flash-based drives, according to the research, which was presented the week of February 21 at the Usenix FAST 11 conference in California. In some cases, the SSDs, or solid-state drives, incorrectly indicate the files have been “securely erased” even though duplicate files remain in secondary locations. The difficulty of reliably wiping SSDs stems from their radically different internal design. Traditional ATA and SCSI hard drives employ magnetizing materials to write contents to a physical location that's known as the LBA, or logical block address. SSDs, by contrast, use computer chips to store data digitally and employ an FTL, or flash translation layer, to manage the contents. When data is modified, the FTL frequently writes new files to a different location and updates its map to reflect the change. In the process, left-over data from the old file, which the authors refer to as digital remnants, remain. Source: http://www.theregister.co.uk/2011/02/21/flash_drive_erasing_peril/

Facebook users subjected to more clickjacking. Facebook users have been subjected to another round of clickjacking attacks that force them to authorize actions they had no intention of approving. The latest episode in this continuing saga, according to Sophos researchers, is a set of campaigns aimed at Italian-speaking users of the social network. The come-ons promise shocking videos about such things as the real ingredients of Coca Cola. Instead, they are forced into registering their approval of the videos using Facebook's “Like” button. Clickjacking is a term that was coined in 2008. It describes attacks that allow malicious Web site publishers, or their users, to control the links visitors click on. They are typically pulled off by superimposing an invisible iframe over a button or link. Virtually every browser is vulnerable, although many come with safeguards that can make exploitation harder. Source: http://www.theregister.co.uk/2011/02/22/facebook_clickjacking_attacks/

41% of organizations not aware of security risks. Forty-one percent of organizations are not well aware of or protected against IT security risks, according to McAfee. Another 40 percent are not completely confident they can accurately deploy countermeasure products thus leaving them at risk. The McAfee report found that to address these concerns, nearly half of all companies plan to spend an average of 21 percent more in 2011 on risk and compliance solutions. Overall, the survey indicated strong growth for risk and compliance products in 2011 with the majority of decision-making executives demanding integrated and automated solutions rather than point products. Source: <http://www.net-security.org/secworld.php?id=10653>

Security researchers find VoIP account cracking botnet. Security researchers from Symantec have identified a piece of malware designed to brute force the password of VoIP accounts in a distributed manner. The trojan, which Symantec describes as a SIP cracker, after the Session Initiation Protocol (SIP) used by VoIP systems, is being installed on computers by Sality. Sality is a family of file infectors with botnet capability that spread by appending their malicious code to executable files, sometimes corrupting them in the process. The Sality botnet is commonly used as a malware distribution platform in a pay-per-install style operation where other cybercriminals pay to have their creations spread. The SIP cracker has been distributed by Sality for months now with few people noticing, and it is noteworthy because it is the first such malware to be found in the wild. The SIP crackers contact their command and control (C&C) server and ask for an IP range to probe. It then performs some checks on IP addresses in that range to determine if any correspond to a SIP server. When a server is identified, the bot tries to register an account on it using a list of usernames and passwords received from the C&C. If any of the attempts is successful, it reports back with the information. Source: <http://news.softpedia.com/news/Security-Researchers-Find-VoIP-Account-Cracking-Botnet-184990.shtml>

New Steam phishing campaign spotted. Security researchers from Sophos warned that Steam users were being targeted in a new phishing attack that produces fake e-mails threatening them with account suspension. The e-mails bear a subject of "Warning! Your steam account will be suspended?" and have a forged "From" field to appear as if they originate from support(at)steampowered(dot)com. The attackers are probably abusing a legit Steam e-mail template, because the body has a well designed header and footer, displaying the Steam and Valve logos. The lure used in this phishing attack is a traditional one, the threat of something happening with the recipient's account. The link included to "reconfirm" the account appears to point to a location on the support(dot)steampowered(dot)com Web site, but in reality take users to a phishing page that tries to steal log-in credentials. Steam is the largest gaming digital distribution platform with more than 30 million monthly active users and more than 1,200 games available for purchase and download. Steam accounts can be valuable to cybercriminals because they can be associated with payment information. Source: <http://news.softpedia.com/news/New-Steam-Phishing-Campaign-Spotted-184984.shtml>

NATIONAL MONUMENTS AND ICONS

(Virginia) Charges filed for fire in Shenandoah National Park. The Virginia Department of Forestry (DOF) said a homeowner is charged with carelessly damaging property by fire in connection with a fire that has been burning since February 19. Officials said the homeowner was negligent in improperly discarding ashes from a wood stove. He will have to pay suppression costs to the Department of Forestry. The fire in Shenandoah National Park has burned nearly 2,000 acres. Investigators with Warren County Fire and Rescue and the Virginia DOF worked together to find the cause of the wildfire. Source: http://www.whsv.com/news/headlines/Charges_Filed_for_Fire_in_Shenandoah_National_Park_116851523.html

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

Fake Twitter notifications lead to rogue pharma sites. A new wave of rogue e-mails posing as official notifications from Twitter and containing links to illegal online pharmacies have landed in people's inboxes during the week of February 20. According to Belgian e-mail security vendor MX Lab, who intercepted some of the messages, the e-mails bear a subject of "Twitter Notification" and purport to come from a @postmaster.twitter.com address. It appears the spammers modified a legitimate Twitter e-mail template in order to make their messages look as valid as possible. Recipients are informed they have pending notifications in their Twitter accounts and an URL is provided to see them. However, the link actually leads to a website selling male enhancement pills, pain killers, and antibiotics. The Web site is part of the "U.S. Drugs" rogue pharmacy chain, one of several affiliate programs that rose to prominence after the fall of "Canadian Pharmacy" in 2010. According to Spamtrackers EU, the U.S. Drugs Web sites are usually hosted on hacked servers and display deceptive elements such as a fake pharmacy license number, fake Verified by Visa logo, or fake Verisign and FDA links. Pharmaceuticals has been the highest ranking spam category throughout in 2010. Users are strongly advised against buying from such websites. The drugs sold can be fake or can contain controlled substances in dangerous amounts, posing serious health risks. In addition, buying from spam carries a very high risk of credit card fraud. Source:

<http://news.softpedia.com/news/Fake-Twitter-Notifications-Lead-to-Rogue-Pharma-Sites-186255.shtml>

Drug shortages cause hospitals to use older types of medicines. Hospitals across the country are running out of key drugs used in surgeries and to treat some diseases, including cancer, causing doctors to turn to older treatments. In some cases, hospitals are paying higher prices to get patients necessary care because wholesalers are hoarding needed medicines. Part of the shortage has been caused by manufacturing issues and quality-control problems at a number of companies as they respond to a U.S. Food and Drug Administration crackdown on drug safety. The issues range from finding toxins and "particulate matter" in medicines, to workers inaccurately filling out the required paperwork to verify drugs and medical devices are safe and effective. About 150 drugs are in short supply, according to the American Society of Health-System Pharmacists. About 60 of those are considered by federal health officials "medically necessary," including medicines used to treat or prevent a serious disease or medical condition. The drug shortage has been exacerbated by consolidation in the pharmaceutical industry. In addition, some drug companies have exited the business of making older, generic injectable drugs, which typically are not as profitable as newer brand-name medicines. Source: <http://www.latimes.com/business/la-fi-drug-shortage-20110221,0,1760241.story>

FDA knew of problems at plant that made tainted wipes. The death of a 2-year-old Houston, Texas boy from a rare infection blamed on contaminated alcohol wipes may be only the first casualty tied to allegedly shoddy sterilization practices by the Triad Group of Hartland, Wisconsin. Since a February 15

UNCLASSIFIED

report by msnbc.com, dozens of people have said they may have been sickened, too. At the same time, government documents obtained by msnbc.com showed U.S. Food and Drug Administration (FDA) inspectors knew about problems with contamination and sterilization at a plant run by the firm as early as July 2009. "Procedures designed to prevent microbiological contamination of drug products purporting to be sterile are not followed," officials wrote in inspection reports. But there is no record the FDA sent warning letters typically used to force firms to comply. During the week of February 14, more than 50 people contacted lawyers representing the boy's parents, who are suing the Triad Group for gross negligence in their son's December 1 death. "We're seeing a wide spectrum of complaints," said the lawyer representing the family. Reported injuries range from superficial skin infections to serious complications, and even one claim of another death. None of the new infections has been confirmed, he added. Another 100 reports of problems with alcohol prep pads have been logged by the FDA since the January 5 recall of Triad products because of potential contamination with the bacteria *Bacillus cereus*, an agency spokesman said. Triad's recall covers all lots of its alcohol prep pads, wipes, and swabs, totaling perhaps hundreds of millions of products sold in the United States, Canada, and Europe. Source: http://www.msnbc.msn.com/id/41694606/ns/health-infectious_diseases/?GT1=43001

(Oregon; Washington) Inoculations recommended for 50 exposed to Vancouver boy sickened by measles. Clark County, Washington health officials have recommended that upward of 50 people get inoculated against measles days after being exposed to a 7-month-old boy sickened by the disease. The baby, too young to receive a routine measles vaccination, flew home to Washington state from India February 13, and may have spread measles to others at Portland International Airport in Portland, Oregon, and two Vancouver, Washington medical offices. "We're continuing to receive calls from people about exposure to measles," said the Clark County Public Health's incident commander. In all, authorities believe about 130 people may have come into the vicinity of the boy at the Evergreen Pediatric Clinic and in the pharmacy/outpatient lab at the Southwest Washington Medical Center February 14. The infant was in the Horizon Airlines terminal, in Concourse A — gates six through 12, and in baggage claim area 2 — between 7:20 p.m. and 9:20 p.m. Source: http://www.oregonlive.com/clark-county/index.ssf/2011/02/inoculations_recommended_for_50_exposed_to_boy_sickened_by_measles.html

(Illinois) First U.S. cowpox infection: Acquired from lab contamination. A student laboratory worker at the University of Illinois, Urbana-Champaign, is the first person in the United States to come down with cowpox, a less dangerous relative of smallpox, and the culprit is lab contamination. Researchers from the U.S. Centers for Disease Control and Prevention (CDC) reported the week of February 7 at the International Meeting on Emerging Diseases and Surveillance in Vienna that the unvaccinated patient was infected by a genetically modified cowpox virus strain in her research lab, one she had never even worked with, by inadvertently handling contaminated materials. Cowpox exists in the wild in Europe and Asia, but is not found in the United States except in research labs. The cowpox patient had declined vaccination since she had no intention of handling the virus, and the lab had not worked on cowpox for 5 years previous to the incident. However, CDC investigators found cowpox DNA in many locations around the lab and in stocks of purportedly harmless virus, although no live poxvirus was found on surfaces. Source: <http://news.sciencemag.org/scienceinsider/2011/02/first-us-cowpox-infection-acquired.html?ref=ra>

UNCLASSIFIED

111 charged in Medicare scams worth \$225 million. Federal authorities charged more than 100 doctors, nurses, and physical therapists in nine cities with Medicare fraud February 17, part of a massive nationwide bust that snared more suspects than any other in history. More than 700 law enforcement agents arrested dozens of people accused of illegally billing Medicare more than \$225 million. The arrests are the latest in a string of major busts in the past 2 years as authorities have struggled to pare the fraud believed to cost the government between \$60 billion and \$90 billion each year. Stopping Medicare's budget from hemorrhaging that money will be key to paying for the Presidential administration's health care overhaul. The Health and Human Services Secretary and Attorney General partnered in 2009 to allocate more money and manpower in fraud hot spots. The February 17 indictments were for suspects in Miami, Los Angeles, Dallas, Houston, Detroit, Chicago, Brooklyn, Tampa, and Baton Rouge. Authorities also announced they were adding strike forces in Chicago and Dallas. Source:

http://news.yahoo.com/s/ap/20110217/ap_on_bi_ge/us_medicare_fraud_bust

TRANSPORTATION

Senate passes broad aviation bill. A broad aviation bill that would advance modernization of the nation's air traffic control system and boost airport construction was approved February 17 by the U.S. Senate. The bill was approved 87-8. Congress has been struggling for more than 3 years to pass an aviation bill that renews Federal Aviation Administration programs and speeds up the transition from an air traffic control system based on World War II-era radar technology to GPS technology. The new air traffic system would allow planes to fly more precise routes between airports, saving time, money and fuel. The satellite technology would update the location of planes every second instead of radar's every 6 to 12 seconds. Pilots would be able to tell not only the location of their plane, but other planes equipped with the new technology as well — something they can't do now. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5gTijzCZ2TvCXsWcDIg3c7DxmY5oQ?docId=70f38871133142569d91a7ae3d5fc259>

WATER AND DAMS

(Maryland; Vermont; Alaska) Footwear blamed for 'rock snot' invasion of Md. streams. Felt-soled fishing boots, of all things, are apparently the latest threat to local fish populations, prompting Maryland to ban the shoes in hopes of stopping an invasive form of algae — appropriately dubbed "rock snot" for its resemblance to yellow-brown mucous — from hurting pristine trout streams, the Associated Press reports. Maryland's Department of Natural Resources plans to prohibit wading with felt soles starting March 21 after discovering that "rock snot," or didymo — a type of algae that coats riverbeds in thick mats — thrives in the shoes' damp fibers and hitches a ride from one body of water to another. Rock snot has found its way across the United States, and as of March 21, Maryland will become the first state to enforce a felt boot ban. It was found in 2008 in Gunpowder Falls north of Baltimore. A western Maryland stream, the Savage River, also has tested positive for the organism, but has not had a rock snot bloom. Similar bans will take effect in Vermont April 1, and in Alaska in 2012. Source:

http://voices.washingtonpost.com/the-buzz/2011/02/footwear_blamed_for_rock_snot.html?hpid=newswell

UNCLASSIFIED

(North Carolina) Richmond County in severe drought. A lack of significant rainfall in recent months has resulted in below normal groundwater levels and stream-flows and less water than needed to replenish reservoirs in parts of North Carolina. Parts of central North Carolina have been thrust into severe drought, including Richmond County. "Richmond County has been in drought since February 1," the public information officer for the division of water resources. "Severe drought is the second worst out of four categories. It means conditions are getting worse, and it could go into extreme drought," she said. "If dry conditions continue to occur, widespread impacts could quickly surface in the next few months as the temperatures begin to gradually increase and the growing season begins," the chairman of the North Carolina Drought Management Advisory Council said. In the Piedmont, 27 counties are in severe drought, and 38 mountain and eastern counties are abnormally dry, according to the North Carolina drought map. Abnormally dry is not a drought category, but means drought could emerge without adequate rainfall. Source:

http://www.yourdailyjournal.com/view/full_story/11464973/article-Richmond-County-in-severe-drought?instance=home_news_lead

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: 701-328-8175
State Radio: 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED